Gefahr von Cyberangriffen in der Arztpraxis wirksam begegnen

Der Präsident des Bundeskriminalamtes (BKA) Holger Münch warnte unlängst auch vor Cyberangriffen auf Arztpraxen. Nach Angaben des BKA in seinem Webauftritt[1] ist Cybercrime eines der sich am dynamischsten verändernden Kriminalitätsphänomene. Täter passen sich flexibel an technische und gesellschaftliche Entwicklungen an, agieren global und greifen dort an, wo es sich aus ihrer Sicht finanziell lohnt. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) möchte dies zum Anlass nehmen und Ihnen aus datenschutzrechtlicher Sicht einige Informationen zum Sachverhalt übermitteln und Sie bitten, diese in geeigneter Form auch Ihren Mitgliedern zur Verfügung zu stellen.

BSI-Lagebericht zu Ransom-Ware

Im Hinblick auf potentielle Gefahren von IT-Angriffen veröffentlicht das Bundesamt für Sicherheit in der Informationstechnik (BSI) jährlich einen BSI-Lagebericht. Der letzte Lagebericht - „Die Lage der IT-Sicherheit in Deutschland 2022“ - warnt generell davor, dass die Gefährdungslage im Cyber-Raum so hoch wie nie sei. Dabei nehmen aktuell als größte Bedrohung im Cyber-Bereich insbesondere Ransomware-Angriffe zu – d. h. Cyber-Angriffe auf Unternehmen, Universitäten und Behörden – mit dem Ziel, Lösegeld zu erpressen. Dabei wird in der Regel eine Art von Malware (Schadcode) übermittelt, die ein System „sperrt“ oder Dateien verschlüsselt. Klicken Sie beispielsweise auf einen mit Malware infizierten E-Mail-Anhang, so kann sich Malware auf Ihrem Gerät ausbreiten.

Zu den Gründen für die hohe Bedrohungslage gibt das BSI anhaltende Aktivitäten im Bereich der Cyber-Kriminalität, Cyber-Angriffe im Kontext des russischen Angriffs auf die Ukraine und in vielen Fällen eine unzureichende Qualität von genutzten IT- und Software-Produkten an[2].

Dissertationsarbeit zur Gefährdungslage durch Cybercrime

Mit dem Thema *„Gefährdungslage deutscher Arztpraxen (als Teil des Gesundheitswesens und der KMU) durch Cybercrime“* befasste sich auch bereits

[1] https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Cybercrime/cybercrime_node.html
[2] siehe dazu: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/221025_Lagebericht.html

2020 eine Dissertationsarbeit von Herrn Dipl.-Math. oec. Stefan Jäger an der Friedrich-Schiller-Universität Jena. Der Autor kam auf Seite 281 (Fazit und Ausblick) zu folgendem Ergebnis: „In der Analyse kristallisierte sich heraus, dass die größte Zahl an Cybersicherheitsvorfällen nicht durch Kriminelle, sondern durch Mitarbeiter und ehemalige Angestellte durch gewolltes oder ungewolltes menschliches Fehlverhalten verursacht werden. Grund ist hierfür oftmals das fehlende Risikobewusstsein für mögliche Konsequenzen und unzureichend geschulte sowie sensibilisierte Angehörige der jeweiligen Einrichtung."

Weiterhin wurde in dieser Arbeit unter Punkt 8.3[3] analysiert:

„(1) Es herrschte zu lang ein zu geringes Risikobewusstsein bzgl. Cybercrime vor, hieraus resultierten mehrere Problematiken:
a. Investitionen in IT-Sicherheit, sei es in Ausstattung, Personal oder Weiterbildungen, fallen zu gering aus.
b. Maßnahmen zur Erhöhung des IT-Sicherheitsniveaus wurden zu spät in hinreichendem Maße ergriffen.
c. Sensibilisierungsmaßnahmen, als Sonderfall von Weiterbildungen, werden auch zum heutigen Zeitpunkt in deutlich zu geringem Umfang durchgeführt.

(2) Fachliche Mitarbeiter sowie Sachbearbeiter im Gesundheitswesen sind zunehmend mit der rasanten Geschwindigkeit überfordert, mit welcher die Digitalisierung in ihrem Arbeitsumfeld voranschreitet und somit die Komplexität erhöht wird. „Daten werden mittlerweile standardmäßig in digitaler Form gespeichert und digital übertragen, zudem kommt eine Vielzahl an zu verwendenden Applikationen zum Einsatz."[4]

Pflicht zur Meldung nach Art. 33 DS-GVO

Gemäß Artikel 33 Abs. 1 Datenschutz-Grundverordnung (DS-GVO) sind Verantwortliche verpflichtet, Verletzungen des Schutzes von personenbezogenen Daten dem TLfDI innerhalb von 72 Stunden nach Bekanntwerden der Verletzung zu melden. Im laufenden Jahr 2023 hat der TLfDI bislang keine Meldungen nach Artikel 33 DS-GVO über Hackerangriffe auf Arztpraxen erhalten. Hingegen wurden dem TLfDI im Tätigkeitsjahr 2022 zwei Cyberangriffe auf Arztpraxen gemeldet. Im Jahr

[3] Ergebnisse auf Seite 274
[4] Für weitergehende Informationen und Erkenntnisse der Dissertation siehe „Gefährdungslage deutscher Arztpraxen (als Teil des Gesundheitswesens und der KMU) durch Cybercrime" unter https://www.db-thueringen.de/servlets/MCRFileNodeServlet/dbt_derivate_00051012/dissjaeger.pdf.

2021 war dem TLfDI ein Cyberangriff auf Arztpraxen bekannt gemacht geworden. Ob und inwiefern darüberhinausgehende Cyberangriffe auf Thüringer Arztpraxen verübt worden sind, ist dem TLfDI mangels entsprechender Meldungen nicht bekannt. Es sei in diesem Zusammenhang darauf hingewiesen, dass eine unterlassene Meldung nach Art. 33 DS-GVO nach Art. 83 Abs. 4 Buchst. a) DS-GVO bußgeldbewehrt ist.

Hinweise des TLfDI

Aus Sicht des TLfDI ist immer ein Angriffspotenzial auf alle Systeme gegeben, wenn diese nicht ausreichend nach den Empfehlungen des BSI technisch und organisatorisch gesichert sind. Spätestens mit dem Lagebericht des BSI von 2022 sollten alle Verantwortlichen aufwachen. Das BSI weist darauf hin, dass die Gefährdungslage im Cyber-Raum hoch wie nie ist. Der TLfDI schließt sich der Auffassung des BSI an, dass Cyber-Sicherheit ein wesentlicher Aspekt der Daseinsvorsorge ist und unmittelbar dem Schutz von Bürgerinnen und Bürgern dient[5].

Gerade im Hinblick darauf erscheint es aus datenschutzrechtlicher Sicht sehr wichtig, dass Arztpraxen die Richtlinie nach § 75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit der Kassenärztlichen Bundesvereinigung (KBV) umsetzen[6], um sich und die personenbezogenen Daten „ihrer“ Patienten ausreichend vor Hackerangriffen zu schützen. Die entsprechende Richtlinie der KBV zur Gewährleistung der IT-Sicherheit enthält in Anlage 1- 5 umfassende Hinweise und Vorgaben zum technischen und organisatorischen Schutz von Patientendaten in kleinen und großen Arztpraxen sowie Anforderungen bei der Nutzung medizinischer Großgeräte und zum Einsatz von Komponenten der Telematikinfrastruktur. Die Kassenärztliche Bundesvereinigung hat nach § 75b SGB V den Auftrag, Anforderungen zur Gewährleistung der IT-Sicherheit in der vertragsärztlichen Versorgung zu regeln. Sie hat damit den Auftrag, den Stand der Technik, also der technischen und organisatorischen Maßnahmen im Sinne von Artikel 32 DS-GVO zu standardisieren. Nach ihrer Präambel erfüllt die Richtlinie diesen Auftrag und dient damit dem Zweck, die Handhabung der Vorgaben der DS-GVO im Zusammenhang mit der elektronischen Datenverarbeitung für die vertragsärztliche Praxis zu vereinheitlichen und zu erleichtern: „Die Richtlinie adressiert die Schutzziele

[5] vgl. Pressemitteilung des BSI vom 25.10.2022, https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/221025_Lagebericht.html
[6] https://www.kbv.de/media/sp/RiLi___75b_SGB_V_Anforderungen_Gewaehrleistung_IT-Sicherheit.pdf

Vertraulichkeit, Integrität und Verfügbarkeit der IT-Systeme in der vertragsärztlichen – psychotherapeutischen Praxis. Die Richtlinie legt technische Anforderungen fest und beschreibt das Mindestmaß der zu ergreifenden Maßnahmen, um die Anforderungen der IT-Sicherheit zu gewährleisten. Mit der Umsetzung der Anforderungen werden die Risiken der IT-Sicherheit minimiert. Bei der Umsetzung können Risiken auch an Dritte, wie IT-Dienstleister oder Versicherungen, übertragen oder durch den Verantwortlichen akzeptiert werden."

Da es sich bei der Verarbeitung von Patientendaten um die Verarbeitung besonderer Kategorien personenbezogener Daten nach Artikel 9 Abs. 1 DS-GVO handelt, sind die verantwortlichen Inhaber der Arztpraxen gemäß Artikel 5 i. V. m. Artikel 32 Abs. 1 DS-GVO verpflichtet, auch dementsprechend umfassende technische und organisatorische Maßnahmen zum Schutz dieser Daten zu ergreifen bzw. implementieren. Die weiter vorn erwähnte Richtlinie zählt dazu z.B. einfache Maßnahmen auf, wie ein sicheres Passwort oder eine PIN zu nutzen, Apps nur aus vertrauenswürdigen App-Stores zu nutzen oder regelmäßige Datensicherungen durchzuführen. Aber auch durchaus nicht triviale Maßnahmen zur Datenverschlüsselung, Absicherung des Netzwerkes der Arztpraxis, die sichere Anbindung an die Telematik-Infrastruktur oder eine differenzierte Vergabe von Nutzerrechten innerhalb der Arztpraxis müssen beachtet werden. Der Katalog ist je nach Praxisgröße unterschiedlich lang und komplex.

Nach Angaben des Thüringer Landesamtes für Statistik gab es zum Stichtag 31.12.2021 2.365 niedergelassene (Privat- und Vertrags-) Ärzte in Thüringen[7]: Wenn eine Meldung nach Artikel 33 DS-GVO beim TLfDI eingeht, wird im Einzelfall geprüft, ob bei diesem konkreten Vorfall die DS-GVO, insbesondere die Verarbeitung nach Artikel 9 DS-GVO ordnungsgemäß umgesetzt und technische und organisatorische Maßnahmen i. S. v. Artikel 32 Abs. 1 zum Datenschutz ergriffen wurden.

Gemäß § 75b Abs. 4 Satz 1 SGB V ist die IT-Richtlinie der KBV für die an der vertragsärztlichen und vertragszahnärztlichen Versorgung teilnehmenden Leistungserbringer verbindlich[8] und von diesen umzusetzen. Aus datenschutzrechtlichen Gründen, insbesondere im Hinblick auf potentielle Hackerangriffe, sollte die IT-Richtlinie jedoch auch von Privatärzten, d. h. nicht an der vertragsärztlichen und

[7] https://statistik.thueringen.de/datenbank/TabAnzeige.asp?tabelle=kr001408%7C%7C
[8] siehe https://www.gesetze-im-internet.de/sgb_5/__75b.html

–zahnärztlichen Versorgung beteiligten Arztpraxen im Interesse der Patienten umgesetzt werden.

Projekt „CyberPraxMed“

Mit dem Projekt „CyberPraxMed“ hat das BSI die Problematik der IT-Sicherheit in Arzt-Praxen im März 2023 selbst auch aufgegriffen. Das Projekt CyberPraxMed hat das Ziel, durch eine Umfrage den Netzwerkaufbau und die Ausstattung typischer Arztpraxen zu erfassen und die Sicherheitsrisiken einzuschätzen. Darüber hinaus soll die Fachexpertise im Bereich der IT-Sicherheit des Personals, der Ärzte und eines gegebenenfalls beauftragten IT-Dienstleisters bestimmt werden. Zusätzlich sollen Korrelationen der IT-Sicherheit mit der Praxisgröße, dem Praxistyp und der geographischen Lage untersucht werden.[9] Ziel des Projektes ist es, durch eine Umfrage den Netzwerkaufbau und die Ausstattung typischer Arztpraxen zu erfassen und die Sicherheitsrisiken einzuschätzen.

Thüringer Landesbeauftragter für den
Datenschutz und die Informationsfreiheit

[9] https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/Lagebild_Gesundheit_230327.html